Cisco Secure Cloud Analytics

2020 年 11 月

© 2020 Cisco and/or its affiliates. All rights reserved.

目次

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Cloud Analytics データシート

このドキュメントでは、Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud Public Cloud Monitoring）の製品概要と注文情報について説明します。

製品の詳細については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html を参照してください。

パブリッククラウドとハイブリッド環境を保護するために必要な可視化と継続的な脅威検出を実現します。

製品の概要

パブリッククラウドに移行する IT リソースが増えるにつれ、クラウド資産を標的とする攻撃者を検出するために必要な可視性が不可欠となっています。さらに、使いやすく、運用効率の高いソリューションも求められています。Secure Cloud Analytics は、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform などすべての主要なクラウド環境でワークロードを高度に保護するために必要な可視性と脅威検出機能を提供します。

また、開発チームは、サーバレスや AWS Lambda、Kubernetes といったコンテナなど、よりダイナミックな新しいコンピューティング環境を継続的に採用しています。Secure Cloud Analytics は、こうした環境にも可視性を提供するため、組織はデジタル変革への道のりでセキュリティを侵害する必要がなくなります。

Secure Cloud Analytics は、包括的な可視性と低ノイズで高精度のアラートを、エージェントを使用せずに提供します。また、組織は、クラウド セキュリティ ポスチャを監視して設定のベストプラクティスと社内ポリシーの遵守を確保し、潜在的なリスクやクラウド インフラストラクチャの露出を制限することもできます。Secure Cloud Analytics は、クラウドベースの Software-as-a-Service（SaaS）で提供されるソリューションです。ランサムウェアやその他のマルウェア、データ漏洩、ネットワークの脆弱性、システム、イベント、設定のリスク、侵害を示すロールの変更を検出します。

クラウド環境の保護に加え、Secure Cloud Analytics は Cisco Secure Network Analytics SaaS（旧 Stealthwatch Cloud Private Network Monitoring）を使用してプライベートネットワークにも拡張でき、単一のダッシュボードを使用してハイブリッド環境の可視化と脅威検出を実現できます。プライベートネットワーク上のコネクテッドデバイスの数が大幅に増加している中、セキュリティ担当者は、環境内で動作しているエンティティについて、組織に脅威をもたらすかどうかはもとよりその内容を把握するのに苦労しています。Secure Cloud Analytics を使用すれば、ネットワーク、クラウド、またはその両方の環境で攻撃が行われているかどうかに関係なく、組織はリアルタイムで脅威を正確に検出できるようになります。

また、Secure Cloud Analytics には、最も包括的で統合的なセキュリティ プラットフォームである Cisco SecureX が付属しています。これにより、可視性の統合、脅威への対応の簡素化、およびあらゆる脅威媒体およびアクセスポイントでの自動化を実現します。

© 2020 Cisco and/or its affiliates. All rights reserved.

機能とメリット

機能	利点
ネットワークおよびクラウド分析	デバイスレベルのネットワークトラフィックと通信パターンの完全に自動化されたリアルタイム分析を提供し、パブリッククラウドおよびプライベートネットワークで動作するすべてのデバイスとリソースを可視化します。
信頼度の高いセキュリティアラート	実用的なインテリジェンスを提供し、誤検出を減らしてこれまで以上にスマートなセキュリティアクションを実現します。
組み込み SecureX プラットフォーム	業界で最も包括的かつ統合的なセキュリティ プラットフォームで、可視性の統合、脅威への対応の簡素化、および自動化を実現します。
リスクとポスチャのモニタリング	業界のベストプラクティスまたは社内ポリシーに沿って、クラウド環境にリスクをもたらす可能性のある不良構成や変化を迅速に特定します。
Software as a Service（SaaS）	組織が大規模にセキュリティを導入する際に必要とされる使いやすさ、導入の容易さ、および柔軟性が強化されます。
エンティティモデリング	ネットワーク上のすべてのデバイスおよびエンティティの動作モデルを提供します。このモデルは、動作の突然の変化や、脅威を示す悪意のあるアクティビティを自動的に識別するために使用されます。
自動ロール分類	動作に基づいて、各ネットワークデバイスとクラウドリソースのロールを自動的に識別します。
エージェントレスの展開	ネットワークおよび Amazon Web Services（AWS）、Microsoft Azure、および Google Cloud Platform（GCP）クラウドインスタンスからのテレメトリのネイティブソースおよびログを使用します。特殊なハードウェアまたはソフトウェアエージェントは必要ありません。
プライベートネットワーク/ハイブリッド環境のモニタリング	セキュリティ運用やワークフローを合理化する単一のツールを使用して、プライベートネットワークおよびパブリッククラウドのリソースに対する脅威や異常を検出します。

最新のネットワークセキュリティ

今日の組織は、セキュリティの「盲点」に悩まされています。プライベートネットワーク上のデバイスが急増し、パブリッククラウドに移行されるワークロードが増えています。一方、セキュリティ担当者には、管理不能な状態になるまでセキュリティアラートが殺到します。シスコ 2019 年 CISO ベンチマーク調査によると、調査対象となったセキュリティアラートは 51% のみで、その半分以上はいまだ修復されていません。

攻撃者はこれらの開発をすぐさま利用してネットワークの防御を突破し、検出をまぬがれます。組織には、ネットワークアクティビティを簡単に確認し、「通常の」エンティティの動作を把握して脅威の兆候を特定する方法が必要です。Secure Cloud Analytics は、パブリッククラウドからテレメトリのソースとログを使用し、動作をモデル化して脅威のアクティビティを特定することでこれを実現します。

可視性と分析

このテレメトリは Secure Cloud Analytics で処理され、プライベートネットワーク、ブランチ、パブリッククラウドなどの最新のネットワークによってアクティブなすべてのエンティティに対する可視性が提供されます。Secure Cloud Analytics は、エンティティモデリングを使用してさまざまな脅威アクティビティを高い精度で検出できます。信頼度の高いセキュリティアラートがよりスマートなセキュリティ判断をサポートし、誤報の数を減らして調査に費やす時間を短縮します。

© 2020 Cisco and/or its affiliates. All rights reserved.

柔軟性と使いやすさ

Secure Cloud Analytics は Software as a Service（SaaS）として提供されるため、試用、購入、利用が容易です。専用ハードウェアを購入する必要がなく、ソフトウェアエージェントの導入や特別な専門知識も不要です。

ソリューションがデータの受信を開始した時点からは、追加の設定やデバイスの分類は必要ありません。すべての分析が自動化されているため、運用に必要な管理およびセキュリティに関する専門知識はほとんど必要ありません。

クラウド セキュリティ ポスチャ管理

Secure Cloud Analytics は、導入時にリスクのある構成や変化についてクラウドリソースのチェックを開始します。独自のウォッチリストを作成して関心のあるアクティビティに対するアラートを生成し、クラウドリソースが社内ポリシーに準拠していることを確認することもできます。

高度な脅威検出のためのエンティティモデリング

テレメトリが収集されると、Secure Cloud Analytics は、ネットワーク上またはモニタ対象のパブリッククラウド内にあるすべてのアクティブエンティティのモデル（一種のシミュレーション）を作成します。このモデリングを使用することで、侵害の初期段階や隠された兆候を迅速に特定できます。更新するシグニチャリストや展開するソフトウェアエージェントはありません。

各モデルは、エンティティ動作の次の 5 つの主要な項目で構成されます。

- **予測：**過去のアクティビティに基づいてエンティティの動作を予測し、これらの予測に対して観測された動作を評価します。
- **グループ：**類似するエンティティと比較することで、エンティティの動作の一貫性を評価します。
- **ロール：**エンティティの動作に基づいてロールを決定し、そのロールと一致しないアクティビティを検出します。
- **ルール：**エンティティが組織のポリシーに違反した場合（プロトコルとポートの使用、デバイスとリソースのプロファイル特性、ブロックリストに記載された通信など）に検出します。
- **一貫性：**データ伝送とアクセスの両方の特性において、デバイスが過去の動作から大きく逸脱したタイミングを認識します。

エンティティモデリングを利用すると、潜在的な脅威に関連するさまざまな動作を検出できます。たとえば、Secure Cloud Analytics ではパブリッククラウドリソースを自動分類します。このリソースの動作では、類似するエンティティの動作との比較が経時的に行われます。これらの通信パターンによって「通常の」動作のベースラインが構築され、このベースラインから逸脱するトラフィックがある場合に、ユーザは電子メールや他のシスコアプリを介してカスタムアラートを受信できます。また、Cisco SecureX プラットフォームまたは他のサードパーティ ソリューションを介して脅威を修復することも可能です。Secure Cloud Analytics は、すべての主要なパブリック クラウド プロバイダーのロールを識別できます。ほぼリアルタイムで新しい動作をすべて検出し、疑わしいトラフィックの詳細とともにアラートを生成します。

DNS の不正使用、地理的に異常なリモートアクセス、永続的なリモート制御接続、および潜在的なデータベースのデータ漏洩は、Secure Cloud Analytics によるアラートの例です。さらに、上位の IP、最も使用されているポート、トラフィックの統計情報を含むアクティブなサブネットなどのネットワークレポートを使用できます。

© 2020 Cisco and/or its affiliates. All rights reserved.

Secure Network Analytics SaaS を使用したプライベートネットワークのモニタリング

前述のように、Secure Network Analytics SaaS を使用すると、ユーザは Secure Cloud Analytics と同じインターフェイスからプライベートネットワークもモニタできるようになります。詳細については、『Cisco Secure Network Analytics Data Sheet』を参照してください。

提供内容

Secure Cloud Analytics

Secure Cloud Analytics は、Amazon Web Services（AWS）、Google Cloud Platform、および Microsoft Azure インフラストラクチャで可視性と脅威検出を提供します。クラウドで提供される SaaS ベースのソリューションで、簡単かつ迅速に導入できます。

ソリューションは、ソフトウェアエージェントを使用する代わりに仮想プライベートクラウド（VPC）のフローログなどテレメトリのネイティブソースに依存して展開できます。Secure Cloud Analytics は、組織のリソースおよび機能によって生成されるすべての IP トラフィックをモデル化します。VPC 内または VPC 間にあるか、外部 IP アドレス宛てであるかは問いません。Cloud Trail、Cloud Watch、Config、Inspector、Identity and Access Management（IAM）、Lambda など追加のクラウド サービス プロバイダー API と統合されます。

注文情報

Secure Cloud Analytics 製品 ID：ST-CL-SUB

ライセンスはサブスクリプションベースで、期間は 1 か月、12 か月、24 か月、36 か月、および 60 か月の中から選択できます。1 か月および 12 か月の自動更新というオプションもあります。期間オプションを選択した後で、パブリック クラウド モニタリングやプライベート ネットワーク モニタリングのサービスを追加できます。

発注の際は、シスコの代理店にお問い合わせください。

セキュリティ向け Cisco Software Support

セキュリティ向け Cisco Software Support の基本的なオンライン サポート オプションは、Secure Cloud Analytics サブスクリプションで利用できます。基本的なオンラインサポートでは、購入したソフトウェア サブスクリプションの全期間にわたって次の基本的なサポートを提供します。

- オンラインツールによるサポートへのアクセス。電話によるサポートは提供されていません。
- シスコは送信されたケースに対し、翌営業日の標準業務時間内までに応答します。

Secure Cloud Analytics のサブスクリプションを注文すると、基本的なオンラインサポートがそのサブスクリプションの一部として組み込まれます。これは個別に注文できるサービスではありません。したがって、Secure Cloud Analytics のサブスクリプションが更新されると、基本的なオンラインサポートも同じ期間で更新されます。SaaS サブスクリプションでこのサポートを受けるにあたって、製品の追加購入や追加料金は不要です。

Cisco Software Support の詳細については、サービスの説明を参照してください。

© 2020 Cisco and/or its affiliates. All rights reserved.

環境を今すぐ保護

リスクのない 60 日間の無料トライアルで、今すぐ Secure Cloud Analytics をお試しください。詳細については、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html を参照するか、お近くのシスコアカウント担当者にお問い合わせください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

©2021 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は2021年2月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-739619-04JA 21.02